CLAIMS

1.   (currently amended) A key management system for controlling access to a vehicle key stored proximal to a remotely located vehicle, comprising:

a key container located proximal to the vehicle, the key container having a key storage area for storing a vehicle key associated with the vehicle and being secured by an electronic lock, the key container having a memory that is ~~capable of~~ operable to ~~recording~~ record information when the key storage area is accessed; and

an electronic key for accessing the key container, the electronic key operable to ~~being capable of establishing~~ establish a wireless communications link with the electronic lock of the key container and having a memory,

wherein information about access events is caused to be stored in ~~at least one of the memory of the key container memory or~~ the electronic key memory during an access or an attempted access for later uploading to a central computer.

2.   (original) The system of claim 1, wherein the wireless communications link is an infrared link.

3.   (original) The system of claim 1, wherein the wireless communications link is an RF link.

4.   (original) The system of claim 1, wherein the electronic key is an open architecture personal digital assistant.

5.   (original) The system of claim 1, wherein the electronic key is an open architecture mobile phone.

6.   (currently amended) The system of claim 1, further comprising a key tag associated with the vehicle key, the key tag having an electronically stored identifier and being detectible by the key container ~~when placed in the key storage area~~ via a wireless communications link.

7.   (currently amended) A key management system for controlling access to vehicle keys, comprising:

a key set that includes a vehicle key to a particular vehicle and a key tag associated with the vehicle key, the key tag having an electronically readable identifier stored thereon and an electrical contact portion;

a key container that can be located on or near the vehicle, the key container having a key set storage area secured by an electronic lock, the key container ~~capable of~~ operable to ~~detecting~~ detect the key set when the key set is properly stored in the key set storage area; and

an open architecture electronic access device carried by a user to access the key container, the access device having a memory that is updated with at least the identifier of the key tag when the key container is successfully accessed and the key set is removed from the key set storage area.

8.   (original) The key management system of claim 7, wherein the key container includes a memory that stores at least the identifier of the key tag of the stored key set.

9.   (original) The key management system of claim 7, wherein the memory of the key container includes a lock out list identifying an unauthorized access device or an unauthorized user.

10.   (original) The key management system of claim 7, wherein the memory of the access device records the approximate time that a successful access was made.

11.   (currently amended) The key management system of claim 7, wherein the memory of the access device records the approximate time that the key tag was returned to the key ~~tag~~ set storage area.

12.   (original) The key management system of claim 7, further comprising a central computer and an associated database for administering the key management system, the central

computer allowing an administrator to set the user's access privileges and track the user's access activity.

13.   (original) The key management system of claim 12, wherein the user logs into the central computer to reestablish his expired access privileges.

14.   (original) The key management system of claim 7, wherein the user seeking to access the key container uses the access device to communicate the user's identifying information and to select one of a predetermined group of codes corresponding to the purpose of the access.

15.   (currently amended) A key management system for controlling access to vehicle keys, comprising:

a key set that includes a vehicle key to a particular vehicle and a key tag associated with the vehicle key, the key tag having an electronically readable identifier stored thereon and an electrical contact portion;

a key container that can be located on or near the vehicle, the key container having a key set storage area secured by an electronic lock, the key container operable to detect the key set when the key set is properly stored in the key set storage area; and

an open architecture electronic access device carried by a user to access the key container, the access device having a memory that is updated with at least the identifier of the key tag when the key container is successfully accessed and the key set is removed from the key set storage area; The key management system of claim 7, wherein the access device is programmed to expire periodically, and wherein information stored in the memory of an expired access device is automatically uploaded to a database.

16.   (original) The key management system of claim 15, wherein the information stored in the memory of an expired access device is automatically uploaded to a database when the access device is reauthorized.

17.   (original) The key management system of claim 7, wherein the key container is ~~capable of communicating~~ <u>operable to communicate</u> with the key set when the electrical contact portion of the key tag is placed to complete an electrical circuit of the key container.

18.   (original) The key management system of claim 7, wherein the key container and access device are each programmed to participate in a challenge response exchange with each other during user attempts to access the key container.

19.   (original) The key management system of claim 7, wherein the access device memory includes stored privileges associated with a specific user to which the access device has been assigned, and wherein at least some of the privileges are set to expire periodically.

20.   (original) The management system of claim 7, wherein the key container memory includes information on access privileges that is used in determining whether the user's access request is granted based on comparing the information on access privileges stored in the key container memory with a specific user's privileges communicated via the access device.

21.   (currently amended) A key management system for controlling access to vehicle keys, comprising:

a key set that includes a vehicle key to a particular vehicle and a key tag associated with the vehicle key, the key tag having a memory having a stored electronically readable identifier and ~~capable of storing~~ <u>operable to store</u> tracking information; and

a key container that can be located on or near the vehicle, the key container having a key set storage area secured by an electronic lock, the key container ~~capable of detecting~~ <u>operable to detect</u> the key set when the key set is properly stored in the key set storage area; and

an electronic access device carried by a user to access the key container, the access device having a memory that is updated with at least the identifier of the key tag when the key container is successfully accessed and the key set is removed from the key set storage area.

22.   (original) The key management system of claim 21, wherein the key container communicates wirelessly with the key tag.

23.   (original) The key management system of claim 21, wherein the key tag and access device are each programmed to participate in a challenge response exchange with each other during user attempts to access the key container.

24.   (original) The key management system of claim 21, wherein the access device memory includes stored privileges associated with a specific user to which the access device has been assigned, and wherein at least some of the privileges are set to expire periodically.

25.   (original) The key management system of claim 21, wherein the key tag memory includes information on access privileges that is used in determining whether the user's access request is granted based on comparing the information on access privileges stored in the key tag memory with a specific user's privileges communicated via the access device.

26.   (currently amended) A key management system for controlling access to a vehicle key stored proximal to a remotely located vehicle, comprising:

a key container located proximal to one of the remotely located vehicles, the key container having a key storage area for storing a vehicle key associated with the respective vehicle and being secured by an electronic lock;

a key tag associated with the vehicle key, the key tag having a memory with an electronically stored identifier and ~~capable of recording~~ operable to record information when the key storage area is accessed; and

an electronic key for accessing the key container, the electronic key ~~being capable of establishing~~ operable to establish a communications link with the key tag via the key container and having a memory,

wherein information about access events is stored in at least one of the memory of the key tag or the memory of the electronic key.

27-31. (cancelled)

32.   (original) A decentralized key management system for controlling access to multiple vehicles among multiple users, the system comprising vehicle keys for the respective vehicles, individual locking key containers for the vehicles, each of the containers having a storage area within which a vehicle key or keys for one vehicle can be stored, electronic access devices for assignment to the users and operable to unlock key containers if authorized, and a database containing information identifying at least the vehicles, the users and access privileges of the users, the access devices being programmable with the information from the database such that a specific user's assigned access device can be programmed with the specific user's access privileges for obtaining access to one or more of the vehicles in the system.